BCH符号（その１）

情報数理学特別講義I 第7回

2025-11-05

今回の講義の目標

$GF(2)$ 上の巡回符号であるBCH符号を知る.
BCH符号が任意の数（少なくとも2個）の誤りをなぜ訂正できるのか.
BCH符号の生成多項式の構成法を学ぶ.

BCH符号の生成多項式を構成するためには以下の知識が必要

- ヴァンデルモンド行列
- 生成多項式の根を用いた巡回符号のパリティ検査行列
- 巡回符号の最小距離
- 最小多項式

今回の講義ではこれらを一つ一つ説明する.

ヴァンデルモンド(Vandermonde)行列とその性質

巡回符号の最小距離に関する定理を理解する上で欠かせない行列であるヴァンデルモンド(Vandermonde)行列とその行列式について説明する.
$x_1, x_2, \ldots, x_n$ を $GF(p^q)$ の元とするとき

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

の形式の行列をヴァンデルモンド行列という.
※ヴァンデルモンド行列は符号理論以外の分野でも出てくる. 例えば離散フーリエ変換の変換行列は要素が複素数のヴァンデルモンド行列となっている.

ヴァンデルモンド行列の行列式

ヴァンデルモンド行列の行列式について，次の定理が成り立つ．

定理 8.1

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le j < i \le n} (x_i - x_j).$$

この定理から導かれる重要な性質：

$x_1, x_2, \ldots, x_n$ が相異なる元であれば行列式が非ゼロになるため，
ヴァンデルモンド行列は正則行列となり逆行列を持つ．

証明

行列式は任意の列の定数倍をある列から引いてもその値は変わらないので，$j \geq 2$ において第 $j-1$ 列のx_1倍を第 j 列から引くことで，ヴァンデルモンド行列の行列式は

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{n-2}(x_2 - x_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n - x_1 & x_n(x_n - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{vmatrix}$$

のように変形できる.

さらに第 1 行について余因子展開することで

$$= \begin{vmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{n-2}(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) & \cdots & x_3^{n-2}(x_3 - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_1 & x_n(x_n - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{vmatrix}$$

が得られる．各 i 行の $(x_{i+1} - x_1)$を係数としてくくり出すと．

$$= (x_2 - x_1)(x_3 - x_1)\dots(x_n - x_1) \begin{vmatrix} 1 & x_2 & x_2^2 & \dots & x_2^{n-2} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} \end{vmatrix} = \prod_{2 \le i \le n} (x_i - x_1) \begin{vmatrix} 1 & x_2 & x_2^2 & \dots & x_2^{n-2} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} \end{vmatrix}$$

上記展開行列に対して，先と同様に$j \ge 2$ において第 $j-1$ 列の x_2 倍を第 j 列から引くことで，

$$= (x_3 - x_2)(x_4 - x_2)\dots(x_n - x_2) \prod_{2 \leq i \leq n} (x_i - x_1) \begin{vmatrix} 1 & x_3 & x_3^2 & \dots & x_3^{n-2} \\ 1 & x_4 & x_4^2 & \dots & x_4^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} \end{vmatrix}$$

$$= \prod_{\substack{2 \leq i \leq n \\ 1 \leq j \leq 2}} (x_i - x_j) \begin{vmatrix} 1 & x_3 & x_3^2 & \dots & x_3^{n-2} \\ 1 & x_4 & x_4^2 & \dots & x_4^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} \end{vmatrix}$$

となる．この操作を繰り返すと，最終的に $\prod_{1 \leq j < i \leq n} (x_i - x_j)$ が得られる．□

練習問題（５分）

原始多項式 $p(x) = 1 + x + x^4$ で定義された $GF(2^4)$ において,
$x_1 = \alpha, x_2 = \alpha^2, x_3 = \alpha^3, x_4 = \alpha^4$
としたときの 4×4 のヴァンデルモンド行列を求めよ.

生成多項式の根を用いた巡回符号のパリティ検査行列

次数 r の生成多項式 $g(x)$ で定義される巡回符号 $\mathcal{C}$ のパリティ検査行列 H は，$g(x)$の根を用いて定義できる．巡回符号の性質より，符号多項式 $c(x)$ は $g(x)$ を因数に持つので，$g(x)$ の r 個の根 $x_1, x_2, \ldots, x_r$ について $c(x_i) = 0$ が成り立つ．
これを行列で表すと，

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_r & x_r^2 & \cdots & x_r^{n-1} \end{pmatrix} \underline{c}^T = \underline{0}$$

となる．ただし $\underline{c} = (c_0, c_1, \ldots, c_{n-1})$ で符号多項式の係数を要素にもつベクトルである．

以上より，巡回符号 $\mathcal{C}$ のパリティ検査行列 H は

$$H = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_r & x_r^2 & \cdots & x_r^{n-1} \end{pmatrix}$$

とかける.

練習問題（５分）

生成多項式 $g(x) = 1 + x + x^4$ で定義される 長さ $n = 15$ の巡回符号 $\mathcal{C}$ のパリティ検査行列 H を$g(x)$ の根 $\alpha \in GF(2^4), p(x) = 1 + x + x^4$ を用いて記述せよ.
ただし，H の記述は以下の２通りで書くこと.

(1) $GF(2^4)$上の元(べき表現でよい)を要素に持つ 1×15 の行列
(2) $GF(2)$上の元を要素に持つ 4×15 の行列

巡回符号の最小距離

定理 8.2
$GF(p)$ 上の長さ $n = p^q - 1$ の巡回符号 $\mathcal{C}$ を考えよう．$\mathcal{C}$ の生成多項式を $g(x), \beta \in GF(p^q)$ を位数 n の元とし，ある非負の整数 a が存在して，$d-1$ 個の連続した指数を持つ $\beta^a, \beta^{a+1}, \ldots, \beta^{a+d-2}$ が $g(x)$ の根であるとする．このとき，巡回符号 $\mathcal{C}$ の最小距離 $d_{\min}(\mathcal{C})$ について $d_{\min}(\mathcal{C}) \geq d$ が成り立つ．

※ガロア体の基礎体の標数を素数 p として書くが，これまでの説明と同様，$p = 2$ と読み替えてかまわない．
※この定理は，符号長が $n = p^q - 1$ を満足しなくても，$GF(p)$ のある拡大体 $GF(p^q)$ に位数 n の元が存在すれば成り立つ．β の位数が n であることは，$\beta^n = 1$ であることを意味する．

証明

$\mathcal{C}$ のパリティ検査行列は生成多項式の根 $\beta^a, \beta^{a+1}, \ldots, \beta^{a+d-2}$ を用いて

$$H = \begin{pmatrix} 1 & \beta^{a} & \beta^{2a} & \ldots & \beta^{(n-1)a} \\ 1 & \beta^{a+1} & \beta^{2(a+1)} & \ldots & \beta^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{a+d-2} & \beta^{2(a+d-2)} & \ldots & \beta^{(n-1)(a+d-2)} \end{pmatrix}$$

とかける.

ここで H の任意の i_1 列, i_2 列, $\ldots$, i_{d-1} 列の $d-1$ 個の列からなる部分行列の行列式を考える.

記述簡略化のため $x_j = \beta^{i_j}$ として,

$$\begin{vmatrix} \beta^{ai_1} & \beta^{ai_2} & \dots & \beta^{ai_{d-1}} \\ \beta^{(a+1)i_1} & \beta^{(a+1)i_2} & \dots & \beta^{(a+1)i_{d-1}} \\ \vdots & \vdots & & \vdots \\ \beta^{(a+d-2)i_1} & \beta^{(a+d-2)i_2} & \dots & \beta^{(a+d-2)i_{d-1}} \end{vmatrix} = \begin{vmatrix} x_1^a & \cdots & x_{d-1}^a \\ x_1^{a+1} & \cdots & x_{d-1}^{a+1} \\ \vdots & & \vdots \\ x_1^{a+d-2} & \cdots & x_{d-1}^{a+d-2} \end{vmatrix}$$

各列の x_j^a を係数としてくくりだすと

$$= x_1^a \cdots x_{d-1}^a \begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_{d-1} \\ \vdots & & \vdots \\ x_1^{d-2} & \cdots & x_{d-1}^{d-2} \end{vmatrix}$$

行列式を求める行列がヴァンデルモンド行列（の転置）であることから，定理 8.1 より

$$= x_1^a \cdots x_{d-1}^a \begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_{d-1} \\ \vdots & & \vdots \\ x_1^{d-2} & \cdots & x_{d-1}^{d-2} \end{vmatrix} = x_1^a \ldots x_{d-1}^a \prod_{i>j} (x_i - x_j) \neq 0$$

となる.

従って，パリティ検査行列の任意の $d-1$ 列は1次独立なので，最小距離は d 以上である.

※パリティ検査行列中のどの $d-1$ 個の列ベクトルを選んでも，その和が $\underline{0}$ にならない.

大切なので再掲

定理 8.2
$GF(p)$ 上の長さ $n = p^q - 1$ の巡回符号 $\mathcal{C}$ を考えよう．$\mathcal{C}$ の生成多項式を $g(x), \beta \in GF(p^q)$ を位数 n の元とし，ある非負の整数 a が存在して，$d-1$ 個の連続した指数を持つ $\beta^a, \beta^{a+1}, \ldots, \beta^{a+d-2}$ が $g(x)$ の根であるとする．このとき，巡回符号 $\mathcal{C}$ の最小距離 $d_{\min}(\mathcal{C})$ について $d_{\min}(\mathcal{C}) \geq d$ が成り立つ．

工学的な意義：t 個の誤りを訂正できる誤り訂正符号を構成可能
任意の誤り数 t を訂正可能な符号に必要な最小距離は $d_{\min}(\mathcal{C}) \geq 2t+1$ である．
定理 8.1 により，t 個の誤りを訂正可能な誤り訂正符号を構成する際に，$2t$ 個の連続した指数を持つ元を根とする生成多項式で定義される巡回符号によりそのような誤り訂正符号が実現できる．

最小多項式の性質

BCH符号を定義するために必要な最後の構成要素である最小多項式について説明する.
なお，ガロア体の基礎体の標数を素数 p として書くが，これまでの説明と同様，$p = 2$ と読み替えていただいてかまわない.

最小多項式：$a \in GF(p^q)$ を根にもち，$GF(p)$ 上の元を係数を持つ最小次数のモニック多項式 $\mu_a(x)$ を元 a の最小多項式（minimum polynomial）と呼ぶ．なお，モニック多項式とは，最高次の係数が 1 である多項式のことである.

- $p = 2$の場合，多項式の引数は $GF(2^q)$ の元だけど，多項式の係数は $GF(2)$ の元.

例

$p(x) = 1 + x + x^4$ で定義された $GF(2^4)$ の原始元 α の最小多項式は $\mu_\alpha(x) = 1 + x + x^4$ である.

最小多項式は次の性質を有する

- 任意の $a \in GF(p^q)$ に対して, a の最小多項式は常に存在する.
- 最小多項式は既約かつ唯一つである.
- $a \in GF(p^q)$ が $GF(p)$ 上の多項式 $f(x)$ の根であるとき，すなわち $f(a) = 0$ であるとき, a の最小多項式 $\mu_a(x)$ は $f(x)$ を割り切る.

定理 8.3
p を素数とするとき，$GF(p)$ 上のある多項式 $\mu(x)$ が a を根として持てば，a^p もまた $\mu(x)$ の根である.

例
$p(x) = 1 + x + x^4$ で定義された $GF(2^4)$ において,
原始元 α の最小多項式 $\mu_\alpha(x) = 1 + x + x^4$ が α^2 も根に持つことを確かめる.
$\mu_\alpha(\alpha^2) = 1 + \alpha^2 + \alpha^8 = 1 + \alpha^2 + (1 + \alpha)^2 = 0.$

証明

簡単のため，$p=2$の場合について証明するが，$p\neq 2$の場合も同様に行える．まず，
$f_1(x), f_2(x) \in GF(2)[x]$とするとき，

$$\left(f_1(x)+f_2(x)\right)^2 = \left(f_1(x)\right)^2 + \left(f_2(x)\right)^2 \tag{8-2}$$

が成り立つことに注意する．

※$GF(2)[x]$ は係数が $GF(2)$ である（$GF(2)$上の）多項式の集合

$\mu(x)$の次数が n で，$\mu(x) = \sum_{i=0}^{n} \mu_i x^i$ とすると，式(8-2)を繰り返し用いることで，

$$
\begin{aligned}
(\mu(x))^2 &= \left(\mu_n x^n + \sum_{i=0}^{n-1} \mu_i x^i \right)^2 = \mu_n^2 x^{2n} + \left(\sum_{i=0}^{n-1} \mu_i x^i \right)^2 \\
&= \mu_n^2 x^{2n} + \left(\mu_{n-1} x^{n-1} + \sum_{i=0}^{n-2} \mu_i x^i \right)^2 \\
&= \mu_n^2 x^{2n} + \mu_{n-1}^2 x^{2(n-1)} + \left(\sum_{i=0}^{n-2} \mu_i x^i \right)^2 \\
&= \mu_n^2 x^{2n} + \mu_{n-1}^2 x^{2(n-1)} + \cdots + \mu_0^2 = \sum_{i=0}^{n} \mu_i^2 x^{2i} = \sum_{i=0}^{n} \mu_i x^{2i} = \mu(x^2)
\end{aligned}
$$

が得られる．ただし，最後から2番目の等式は $\mu_i \in GF(2)$ から $\mu_i^2 = \mu_i$ が成り立つことを用いた．従って，$\mu(a) = 0$ ならば，$\mu(a^2) = (\mu(a))^2 = 0$ である．□

定理 8.4
a を $GF(p^q)$の元とするとき，a の $GF(p)$ 上の最小多項式 $\mu_a(x)$ は

$$\mu_a(x) = (x-a)\left(x-a^p\right)\left(x-a^{p^2}\right)\ldots\left(x-a^{p^{l-1}}\right)$$

で与えられる．ただし，l は $a^{p^l} = a$ をみたす最小の正の整数である．特に，$a \in GF(p^q)$から $a^{p^q} = a$ が成り立つので，$l \leq q$ である．

証明：
ここでも $p = 2$ の場合について証明する．a の $GF(2)$ 上の最小多項式 $\mu_a(x)$ の根は，定理 8.3 から $a, a^2, a^4, \ldots, a^{2^{l-1}}$ である．これから $\mu_a(x)$ の次数が最小であることがわかる．

次に，$\mu_a(x) \in GF(2)[x]$ **（多項式の係数が$GF(2)$の元）であること**を示そう．$GF(2^q)$の標数が2であり，任意の $a \in GF(2^q)$ に対して

$$(x-a)^2 = x^2 - a^2 \tag{8-3}$$

が成り立つことに注意して，$(\mu_a(x))^2$を計算すると，

$$\begin{aligned}
(\mu_a(x))^2 &= (x-a)^2\left(x-a^2\right)^2\left(x-a^4\right)^2 \ldots \left(x-a^{2^{l-1}}\right)^2 \\
&= \left(x^2-a^2\right)\left(x^2-a^4\right)\left(x^2-a^8\right) \ldots \left(x^2-a^{2^{l-1}}\right)\left(x^2-a^{2^l}\right) \\
&= \left(x^2-a^2\right)\left(x^2-a^4\right) \ldots \left(x^2-a^{2^{l-1}}\right)\left(x^2-a\right) \\
&= \mu_a\left(x^2\right)
\end{aligned} \tag{8-4}$$

が得られる．ただし，最後から2番目の等号は，l の定義である $a^{2^l} = a$ を用いた．

ここで，$\mu_a(x) = \sum_{i=0}^{n} \mu_i x^i$とすると，式(8-3)と同様に$a, b \in GF(2^q)$ に対して
$(a+b)^2 = a^2 + b^2$ が成り立つことから，

$$(\mu_a(x))^2 = \sum_{i=0}^{n} \mu_i^2 x^{2i}$$

が得られる．この式と式 (8-4) を組み合わせることで，

$$\sum_{i=0}^{n} \mu_i x^{2i} = \mu_a(x^2) = (\mu_a(x))^2 = \sum_{i=0}^{n} \mu_i^2 x^{2i}$$

が得られる．両端の多項式の各次数の係数を比較することで，$\mu_i^2 = \mu_i \ \ (i = 0, 1, \ldots, n)$が成り立ち，$\mu_i$ は $x^2 = x \Leftrightarrow x(x-1) = 0$ の根なので，$\mu_i \in GF(2)$であることがわかる．従って
$\mu(x) \in GF(2)[x]$である．□

例： 原始多項式 x^6+x+1 の根を α とし，この既約多項式によって定まる有限体 $GF(2^6)$を考える．このとき，$\beta=\alpha^3\in GF(2^6)$の位数は21であり，
β の $GF(2)$ 上の最小多項式 $\mu_\beta(x)$ は，$\beta^{2^5}=\beta^{32}=\beta^{11}$，$\beta^{2^6}=\beta^{64}=\beta$から

$$\begin{aligned}\mu_\beta(x)&=(x-\beta)\left(x-\beta^2\right)\left(x-\beta^4\right)\left(x-\beta^8\right)\left(x-\beta^{16}\right)\left(x-\beta^{32}\right)\\&=\left(x-\alpha^3\right)\left(x-\alpha^6\right)\left(x-\alpha^{12}\right)\left(x-\alpha^{24}\right)\left(x-\alpha^{48}\right)\left(x-\alpha^{33}\right)\\&=x^6+x^4+x^2+x+1\end{aligned}$$

となる．他方 $\beta^3(=\alpha^9)$ の $GF(2)$ 上の最小多項式 $\mu_{\beta^3}(x)$は，
$(\beta^3)^{2^2}=\beta^{12}$，$(\beta^3)^{2^3}=\beta^{24}=\beta^3$から

$$\begin{aligned}m_{\beta^3}(x)&=\left(x-\beta^3\right)\left(x-\beta^6\right)\left(x-\beta^{12}\right)\\&=\left(x-\alpha^9\right)\left(x-\alpha^{18}\right)\left(x-\alpha^{36}\right)\\&=x^3+x^2+1\end{aligned}$$

となる．

位数（order）

※演習に向けた補足として改めて説明

元 $a \in GF(p^q)$ の位数とは，$a^s = 1$ となる最小の $s > 0$ を a の位数と呼ぶ.

- $GF(2^q)$ の原始元 α の位数は $2^q - 1$ である.

例：$GF(2^4)$ において，原始元 α の位数は 15 である．一方 α^3 の位数は 5 で，α^5 の位数は 3 である．重要な性質として，$GF(p^q)$ の元の位数は必ず $p^q - 1$ を割り切る（つまり約数となる）.

演習

生成多項式 $g(x) = 1 + x + x^4$ で定義される符号長15の2元巡回符号に関して，次の問いに答えよ.
(1) この符号の生成行列 G を求めよ.
(2) この符号のパリティ検査行列 H を求めよ.

$p(x) = 1 + x + x^4$ で定義された $GF(2^4)$ における以下の最小多項式を求めよ.
(3) 元 α^3 の最小多項式 $\mu_{\alpha^3}(x)$.
(4) 元 α^5 の最小多項式 $\mu_{\alpha^5}(x)$
ただし最小多項式は因数分解された積形式ではなく，展開した和形式で書くこと.

課題(3)(4)に関する補足説明

積形式から和形式への展開について

> $p(x) = 1 + x + x^4$ で定義された $GF(2^4)$ における以下の最小多項式を求めよ.
> (3) 元 α^3 の最小多項式 $\mu_{\alpha^3}(x)$.
> (4) 元 α^5 の最小多項式 $\mu_{\alpha^5}(x)$
> ただし最小多項式は因数分解された積形式ではなく，展開した和形式で書くこと.

積形式と和形式

積形式とは

$$(x-a)(x-b)$$

のように根の1次式の積で表される形式を指します.
最小多項式は定理8.4にあるように積形式で求めることができます.

和形式とは

$$x^2-(a+b)x+ab$$

のように積形式を展開した多項式を指します.
課題(3)(4)はこの和形式を解答にしてください.

ヒント

やり方としては，まず定理8.4に従い積形式で最小多項式を求めます.
次にその積形式を展開して和形式にします.

なお，最小多項式の係数はすべて $GF(2)$ の元であることに注意してください.
一方で，積形式における根は $GF(2^4)$ の元であることに注意してください.
先の例で言えば a, b は $GF(2^4)$ の元ですが，$a+b$ や ab は $GF(2)$ の元（1 か 0）になります.